

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

United States of America

v.

IONEL MORESANU

Defendant(s)

Case No. 18-843 M(N)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 16, 2018 in the county of Oshkosh in the
Eastern District of Wisconsin, the defendant(s) violated:

Code Section

18 USC 1028(A)
18 U.S.C. 1029(a)

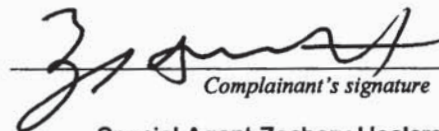
Offense Description

Aggravated Identity Theft
Fraud and related activity in connection with access devices

This criminal complaint is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.


Complainant's signature

Special Agent Zachary Hoalcraft, USSS

Printed name and title

Sworn to before me and signed in my presence.

Date:

June 1, 2018

City and state:

Milwaukee, Wisconsin


Judge's signature

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Zachary M. Hoalcraft, Special Agent, of United States Secret Service, being duly sworn and under oath state the following:

1. I am a Special Agent with the United States Secret Service and have been continuously employed as a Special Agent for approximately five months. I am currently assigned to the Milwaukee, Wisconsin office. Prior to this position, I was a Uniform Division Officer with the United States Secret Service for over two years. I have been involved in security details, patrol investigations involving criminal conduct. I have received formal and on-the-job training regarding counterfeit currencies, frauds, counterfeit debit cards, ATM skimming schemes, and other matters within the jurisdiction of the United States Secret Service.

2. This affidavit is made in support of the issuance of a criminal complaint and arrest warrant against IONEL MORESANU, DOB: 04-14-2000, a Romanian National with no legal status in the United States who is currently in deportation/removal proceedings. Since this affidavit is submitted only for the sole purpose of securing the criminal complaint and arrest warrant, I have not set forth each and every fact known to me concerning this investigation. I have included what I believe are facts sufficient to establish probable cause for the complaint and arrest warrant sought. All of the information contained herein is based upon my personal knowledge, and investigation, or upon information supplied to me by other law

enforcement officers, or private citizens, all of whom I believe to be truthful and reliable.

3. Based on my training and experience, and information obtained from other law enforcement officers who investigate access device fraud and identity theft, I am aware of the following:

4. "ATM skimming" is a scheme in which those involved in this type of criminal activity place a magnetic card reading device, which is usually disguised to look like a part of the ATM, over/into an ATM's actual card reading device. As a customer inserts their credit or debit card into the ATM, the device scans and captures the customer's card account number. As part of the scheme, those involved in this type of criminal conduct also install a pinhole camera, which is usually disguised to look like part of the ATM, to record the customers as they enter their personal identification number (PIN) into the ATM.

5. The device and the pinhole camera can be used to collect hundreds of "skimmed" debit credit card numbers and PINs from unknowing victims. After a period, those involved in "ATM skimming" return to the ATM machines and retrieve the "skimmer" and pinhole camera, which contain the stolen debit card numbers and PINs.

6. After a skimming device and pinhole camera are retrieved, those involved in this skimming scheme use a digital device, such as a laptop, tablet, or mobile phone, to retrieve the stolen debit card account numbers captured on the digital memory of the skimming device. In addition, those involved in this scheme also review video

recorded by the pinhole camera of victims entering their PIN onto the ATM keypad and match the PIN numbers to the debit card account numbers. Therefore, those involved in this type of scheme must use care to review the videos of the transactions in sequential order so that the PIN numbers retrieved correspond to the appropriate debit card numbers.

7. Once this information is obtained, those involved in the scheme re-encode the victims' stolen debit card numbers onto a counterfeit debit card(s) using a magnetic stripe card encoder (also known as a "reader/writer") connected to a digital device, such as a computer or tablet. This encoding converts a blank magnetic stripe card into a counterfeit access device.

8. I know from my training and experience that the creation of counterfeit access devices results in the numbers encoded on the mag stripes of the counterfeit access devices not being the same as those found on the pre-printed account numbers embossed on the front of the cards.

9. Once those involved in the scheme have completed the creation of such a counterfeit access device, they then create a mechanism to be sure to have the correct PIN number associated with the true debit account closely available to the card. Often, those involved in such a scheme will hand-write the PIN number on the counterfeit access device itself, for later use. This is a multi-step process, which is not easily accomplished in a public place without being detected.

10. The act of retrieving compromised debit card accounts from skimming devices, reviewing pinhole camera footage, and re-encoding stolen debit card account

numbers onto counterfeit access devices is most often accomplished in a residence, hotel room, or mini-storage unit.

11. Counterfeit access devices and raw materials used in their creation, are easily hidden by those involved in these schemes in vehicles, hotel rooms, storage units, their residence, and personal belongings. Counterfeit access devices are frequently "hidden" in these areas by these individuals in such a way to decrease the odds of discovery by law enforcement.

12. "ATM skimming" related conspiracies are often highly organized with actors that operate within an organization. Some of the conspirators perform the "on the ground" criminal activity such as installing skimming devices, withdrawing skimming devices, or making fraudulent ATM withdrawals. Often, others perform different tasks, such as downloading the stolen debit card account numbers and PINs from successfully placed skimming devices, encoding stolen debit card numbers onto magnetic stripe cards, and yet others may teach other conspirators how to execute their tasks without being detected by law enforcement.

13. It is common for individuals involved in access device fraud, "ATM skimming" schemes, and identity theft to use digital devices in furtherance of their scheme(s).

14. These digital devices include, but are not limited to, thumb drives, memory chips, flash drives, computers, tablets, cellphones, etc. These individuals use such devices to store information about their access device and identify theft crimes long after the crimes have been committed.

15. This information can include, but is not limited to, the following: addresses and pictures of locations where skimming devices have been installed (to aid co-conspirators in later locating the devices for retrieval); stolen debit card account numbers and PINs; video of victims entering their PINs; ledgers accounting for the proceeds of the scheme; logs of fraudulent transaction histories; funds received; identities of individuals and companies that have been victimized; payments from other co-conspirators; and victim profiles.

16. Such "profiles" may contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and/or employer or taxpayer identification numbers along with other identifying numbers.

17. Individuals who participate in these schemes often maintain telephone numbers and other contact information of their co-conspirators in order to facilitate their crimes together. These individuals will often maintain the contact information and written communications in their cellular telephones and other digital devices.

18. Over the past several months, law enforcement has been investigating a group of Romanians involved in such an "ATM skimming" scheme. This group, which includes IONEL MORESANU, DOB 04/17/2000 (hereinafter "MORESANU"), made unauthorized withdrawals from ATMs in various states including: Tennessee, Georgia, Missouri, Kentucky, Illinois, and Wisconsin using the counterfeit access devices created from the stolen debit and/or credit card information and the stolen PINs from unknowing victims.

19. Videos obtained from various ATM machines in Tennessee captured the installation of the ATM skimming devices, as well as images of several co-conspirators, including MORESANU, making withdrawals from an ATM machine at the First Tennessee Bank in Tennessee using the counterfeit access devices. MORESANU was captured in video surveillance which indicated that he was using a white minivan bearing a Tennessee license plate of 1K0-6J3.

20. On May 16, 2018, Oshkosh Police Department detectives received information from a US Postal Inspector in Nashville, Tennessee that a group of Romanian nationals believed to be responsible for deploying skimming devices and ATM counterfeit access devices across the Midwest were currently staying at the Motel 6 in Oshkosh. The Oshkosh police officers were also informed that one of the vehicles used by this group was a white minivan bearing a Tennessee license plate of 1K0-6J3.

21. Law enforcement went to the Motel 6 and observed a white minivan bearing a Tennessee plate number 1K0-6J3 in the parking lot of the Motel 6.

22. At approximately 8:15 p.m., law enforcement surveilled this minivan travel from the Motel 6 to the Kwik Trip gas station located at 1725 W. 9th Avenue, in the City of Oshkosh, Wisconsin.

23. One of the law enforcement officers covertly entered the Kwik Trip in an attempt to locate the driver and passengers of the minivan. The law enforcement officer observed three males from the van exit the restroom and proceed to the two ATMs in the store. All three of the males were crowded around the machines and appeared to be using the two ATM machines simultaneously. The law enforcement officer observed

them get a receipt for a transaction and then immediately start another transaction. This process continued for several minutes.

24. The law enforcement officer approached them and in order to get a closer view, asked the man if she could use one of the machines. The three individuals stepped aside and continued to use just one of the ATMs. The law enforcement officer observed that they continued to make multiple transactions on what appeared to be different cards. The cards were kept in the possession of a male in a white jogging jacket, whom was later identified as being MORESANU.

25. The law enforcement officer decided to wait for the three individuals outside the store. When the three individuals came out of the store, the law enforcement officer identified herself as a police officer and asked them to stop. One male immediately fled to the west of the store and was apprehended by another law enforcement officer.

26. The man in the white jogging jacket, later identified as MORESANU, stripped himself of a satchel-type purse he was carrying and took off running toward the back of the Kwik Trip store and fled through the back.

27. MORESANU then attempted to climb a wrought-iron fence but was unsuccessful. He turned and squared off with the law enforcement officer whom had watched them in the store and she un-holstered her firearm and told MORESANU to get to the ground. MORESANU was ultimately taken into custody.

28. Recovered from the satchel MORESANU had in his possession, among other items, was an Italian identification card belonging to A.G., dob 4/14/1995; a

Romanian passport in MORESANU's name, with dob 04/14/2000; a Romanian passport belonging to A.M., dob 01/20/2005; miscellaneous receipts; and 80 different counterfeit access devices. These counterfeit access devices had colored stickers on the face of the cards that had bank names written on them and suspected PINs written on the stickers.

29. MORESANU made a statement to law enforcement after he was advised of his rights. He admitted that he used commercially available "Vanilla gift cards" which were encoded with stolen account information in the City of Oshkosh on at least two occasions, including May 15, 2018 and May 16, 2018. He indicated that he received these counterfeit access devices containing stolen information from a boss of the operation to use at various ATMs to withdraw as much money as possible on each visit.

30. MORESANU indicated he usually withdrew \$300-400 per card. Further, MORESANU reviewed with law enforcement officers the surveillance video taken from an incident in Nashville, Tennessee where individuals used cloned ATM cards at a First Tennessee Bank ATM. He identified himself and another individual involved in this scheme as being in that video.

31. MORESANU admitted to flying from Los Angeles to Atlanta on May 11, 2018. MORESANU then drove to St. Louis and obtained 120 counterfeit access devices from another co-actor.

32. MORESANU admitted that he knew that two other individuals had previously placed a skimming device in the St. Louis area to collect account information to be used to produce counterfeit access devices. He also knew that the skimming

devices and the stolen data had been collected and used to create additional counterfeit access devices by others involved in this scheme.

33. MORESANU stated that he took 120 cards from the counterfeit access devices and went to ATMs all over the St. Louis area where he swiped the counterfeit access device, enter the provided PIN, checked the balance, and then withdraw between \$300 and \$400 per counterfeit access device.

34. MORESANU stated he would conduct these transactions on Saturday, Sunday, and early Monday before banks would open. He stated that this particular batch of counterfeit access devices did not yield as much money as usual and that he only received approximately \$5,000. He indicated that one of his co-conspirators was able to obtain between \$7,000 and \$8,000 using the counterfeit access devices he was using, during the same time period.

35. MORESANU stated that after their time in St. Louis, he and several other Romanians in the group went to Oshkosh, Wisconsin. When asked about the counterfeit access devices used in Oshkosh, MORESANU admitted to withdrawing cash from an ATM on May 16, 2018. He further admitted that he used a person's bank account information on a reloadable card on May 15, 2018 to make a purchase of several hundred dollars-worth of snacks and drinks from a Kwik Trip.

36. MORESANU further advised that his next job was scheduled for Louisville, Kentucky and he was supposed to be there by May 19, 2018. He further stated that, as part of the pre-determined plan, he and his co-conspirators were

supposed to drive the minivan to St. Louis, and switch to a different vehicle that his organization had left for him to take to Louisville, Kentucky.

37. On May 16, 2018, I responded to the Oshkosh Police Department to interview MORESANU. MORESANU was again advised of his Miranda Rights, after which he agreed to speak with law enforcement. During the interview, MORESANU stated, in essence, that he was part of an organization that took part in ATM cash out and "ATM skimming" operations across the country.

38. On May 21, 2018, law enforcement conducted a review of some of the counterfeit access devices recovered from MORESANU. Through the use of the Electronic Recovery and Access to Data card reader, law enforcement was able to confirm that the account numbers encoded on the magnetic stripes of the counterfeit access devices were different from the account numbers embossed on the front of the cards, consistent with other "ATM" skimming schemes (see paragraph 7 and 8 above).

39. Law enforcement has already contacted several individuals whose personal financial information was recovered from the counterfeit access devices in MORESANU's possession. Those individuals stated that they had not authorized the use of their personal financial data, had not authorized the withdrawals from their accounts, and did know MORESANU.

###